IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. CONOR BRIAN FITZPATRICK, a/k/a "Pompompurin" Defendant.	**UNDER SEAL** No. 1:23-mj-67

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, John Longmire, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. CONOR BRIAN FITZPATRICK ("FITZPATRICK") is a 20-year-old citizen of the United States, who resides in Peekskill, New York.

2. From at least in or around March 2022 through the present, FITZPATRICK has facilitated the unauthorized purchasing and selling of stolen identification documents, unauthorized access devices, unauthorized access to victim computer systems, and login credentials through his operation of a data breach website named "BreachForums." FITZPATRICK's victims have included millions of United States citizens, as well as a U.S. company providing electronic healthcare services ("Victim-1"), a U.S. company providing internet hosting and security services ("Victim-2"), and a U.S.-based investment company ("Victim-3"), among others.

3. As detailed below, I am submitting this affidavit in support of a criminal complaint and arrest warrant charging FITZPATRICK with conspiracy to commit and aid and abet solicitation for the purpose of offering unauthorized access devices, in violation of 18 U.S.C. §§

1029(a)(6) and 2, all in violation of 18 U.S.C. § 1029(b)(2), in connection with his operation of BreachForums and his middleman service on BreachForums.

4. The evidence below establishes that FITZPATRICK is the user of the moniker "pompompurin" and the main administrator of BreachForums.

AGENT BACKGROUND

5. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for over 16 years. I am currently assigned to the FBI's Washington Field Office Cyber Task Force, where I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for cyber-crimes, including, cyber intrusions, online money laundering, criminal cryptocurrency usage, and criminal online forums.

6. During my career, I have used a number of investigative techniques, including: (a) conducted, monitored, and reviewed physical and wire surveillance, including Title III wiretap investigations; (b) executed search warrants at locations where records of criminal activity have been found, including on electronic devices; (c) reviewed and analyzed numerous recorded conversations and other documentation of criminal activity; (d) debriefed cooperating defendants and confidential human sources; (e) monitored wiretapped conversations; (f) conducted surveillance of individuals engaged in various crimes; and (g) led and participated in search warrants and arrest warrants for various crimes.

7. The facts in this affidavit come from my personal observations, my training and experience, my review of physical and documentary evidence, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

A. Background on Investigation

8. Since in or around March 2022, the FBI, the U.S. Secret Service ("USSS"), and the U.S. Department of Health & Human Services, Office of Inspector General ("HHS-OIG"), collectively, the "U.S. authorities," have investigated an administrator and certain members of a data breach website named "BreachForums" that operates as a popular marketplace for cybercriminals to buy, sell, and trade hacked or stolen data and other contraband, including stolen access devices, means of identification, hacking tools, breached databases, and other services for gaining unauthorized access to victim systems. Among other things, BreachForums enables its members to post solicitations concerning the sale of hacked or stolen data, exchange direct private messages with prospective buyers and sellers, buy access to certain hacked or stolen data that the platform itself controls and distributes, and arrange other services related to the illicit transfer of stolen data and contraband.

B. Background on RaidForums

9. In a separate investigation, the FBI and USSS investigated administrators and users of a website named "RaidForums" for committing and aiding and abetting, *inter alia*, violations of 18 U.S.C. §§ 1028A and 1029 from at least as early as in or around June 2016. According to evidence obtained during the investigation, while active, RaidForums was a popular marketplace for cybercriminals to buy, sell, and trade contraband, including stolen access devices, means of identification, hacking tools, breached databases, and other illegal services.

10. On or about May 6, 2021, a federal grand jury in the Eastern District of Virginia returned a six-count indictment charging Diogo Santos Coelho, RaidForums' alleged founder and chief administrator, with one count of access device conspiracy, in violation of 18 U.S.C.

§ 1029(b)(2), four counts of access device fraud and aiding and abetting the same, in violation of 18 U.S.C. §§ 1029(a) and 2, and one count of aggravated identity theft, in violation of 18 U.S.C. § 1028A(1).

11. On or about January 31, 2022, United Kingdom authorities arrested Coelho pursuant to a request from the United States. A grand jury in the Eastern District of Virginia then returned a six-count second superseding indictment on or around March 15, 2022, that, among others, amended the access device conspiracy count to plead the enhanced sentencing provision of 18 U.S.C. § 3559(g)(1). Coelho remains in the United Kingdom pending the resolution of the United States' request for his extradition.

12. In or around February 2022, the FBI, USSS, and international law enforcement partners took additional steps to prevent RaidForums from operating as a marketplace for illicit material. For instance, on or about February 18, 2022, the Honorable Theresa Carroll Buchanan, Magistrate Judge, issued search warrants (Nos. 1:22-sw-105-107) authorizing the FBI to seize domains that RaidForums used to host the RaidForums website. Authorities in a European country also seized the back-end servers for the RaidForums website in late February 2022.

C. BreachForums Replaces RaidForums

13. After RaidForums' disruption, the FBI observed that a new website accessible at the domain breached.co named "Breached" had been launched in or around March 2022. The website closely resembled RaidForums and appeared to also support the buying and selling of hacked or stolen data. Notably, on or around March 21, 2022, I observed a thread with the subject "Welcome" in which a former RaidForums member with the online moniker "pompompurin" introduced BreachForums as a replacement for RaidForums. The "pompompurin" account is displayed as an "Administrator" account on BreachForums.

14. On or about March 16, 2022, on the website dataknight.org, an individual using the moniker "Lander" posted an apparent interview with pompompurin under the title "Exclusive Interview with 'Pompompurin' about 'Breached'" at https://dataknight[.]org/exclusive-interviewwith-pompompurin/. In this interview, pompompurin reportedly claimed to have created a new website known as "BreachedForums" to fill the void created by the disruption of RaidForums:

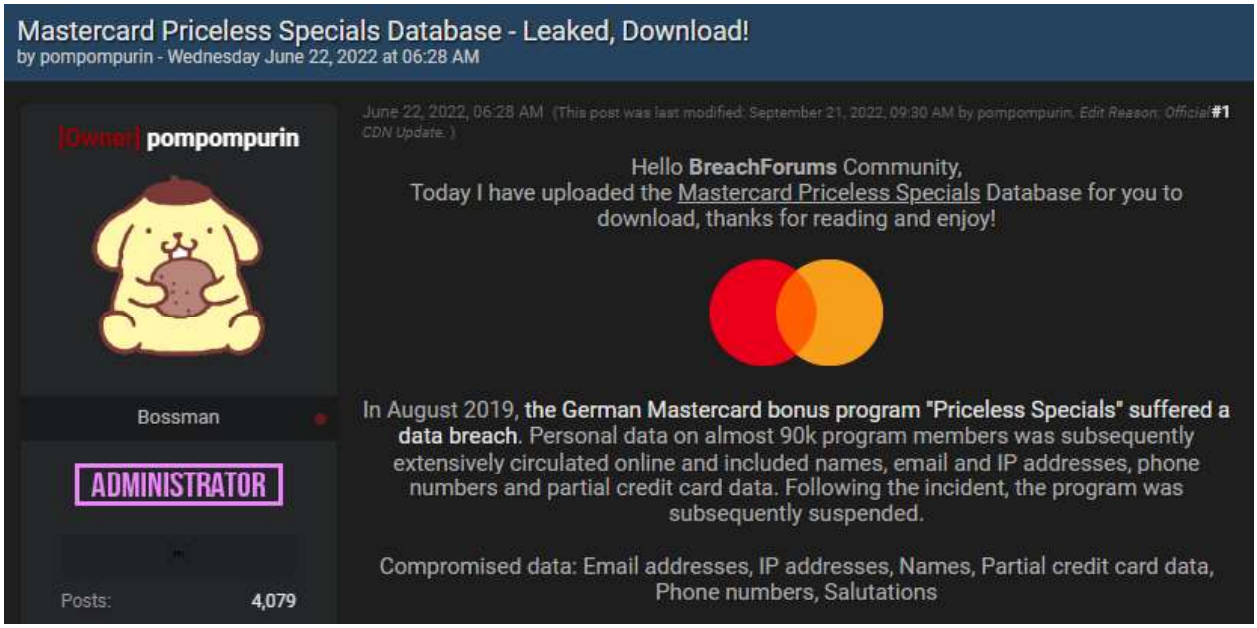
> Conversation:
> Alex – Pseudonym of Lander
> Pom – Shortened version of their moniker
>
> [. . .]
> **Alex**: So to get right into it, What made you want to start BreachForums? Does the closing of RaidForums have anything to do with it
>
> **Pom**: The only reason it's been created was because RaidForums closed, I wouldn't have made it otherwise. The community needs someplace to congregate on and there are no forums similar to what RaidForums offered currently
> [. . .]
> **Alex**: I can see that you've put a lot of work into this… but don't you think that there's a reason that the FBI took down RaidForums? Why would you want to bring it back up knowing that you may face that same fate whatever it [may be]
>
> **Pom**: [Redacted], it doesn't really bother me. If I get arrested one day it also wouldn't surprise me, but as I said I have a trusted person who will have full access to everything needed to relaunch it without me. This person will also never be made known to the public, so it wouldn't be possible for the police to also target them in the event that they want to get the forum taken down for good.
> [. . .]

15. Since its inception, the FBI's review of the BreachForums website indicates that, as with RaidForums, it operates a "Marketplace" section that is dedicated to the buying and selling of hacked or stolen data, tools for committing cybercrime, and other illicit material, including a "Leaks Market" subsection. Some of the items that are commonly sold on BreachForums include bank account information, social security numbers and other PII, and account login information

for compromised online accounts, such as usernames and passwords to access accounts with service providers and merchants. Based on my training and experience, sellers in these marketplaces are typically malicious cyber actors and/or their co-conspirators seeking to monetize data that they obtained through unlawful network intrusions. Buyers in these marketplaces are typically criminal actors who purchase confidential business, financial, or personal data to further other fraud schemes.

16. The BreachForums website has also supported additional sections in which users post stolen or hacked personal identifying information (PII) and discuss tools and techniques for hacking and exploiting hacked or stolen information, including in the "Cracking," "Leaks," and "Tutorials" sections. The BreachForums website also includes a "Staff" section that appears to be operated by the BreachForums administrators and moderators.

17. The BreachForums website does post a "Rules and Policies" section that proscribes the posting or selling of certain classes of material, including a rule stating that the "Selling or Posting Credit/Debit cards is not allowed, and will result in you being banned instantly." However, the FBI's investigation indicates that this rule is often not enforced. For instant, the FBI's review of BreachForums posts reveal numerous posts advertising the availability of payment card information, including several in the "Official" databases section, as further described below. Further, on or about June 22, 2022, "pompompurin" posted a database of compromised Mastercard information:

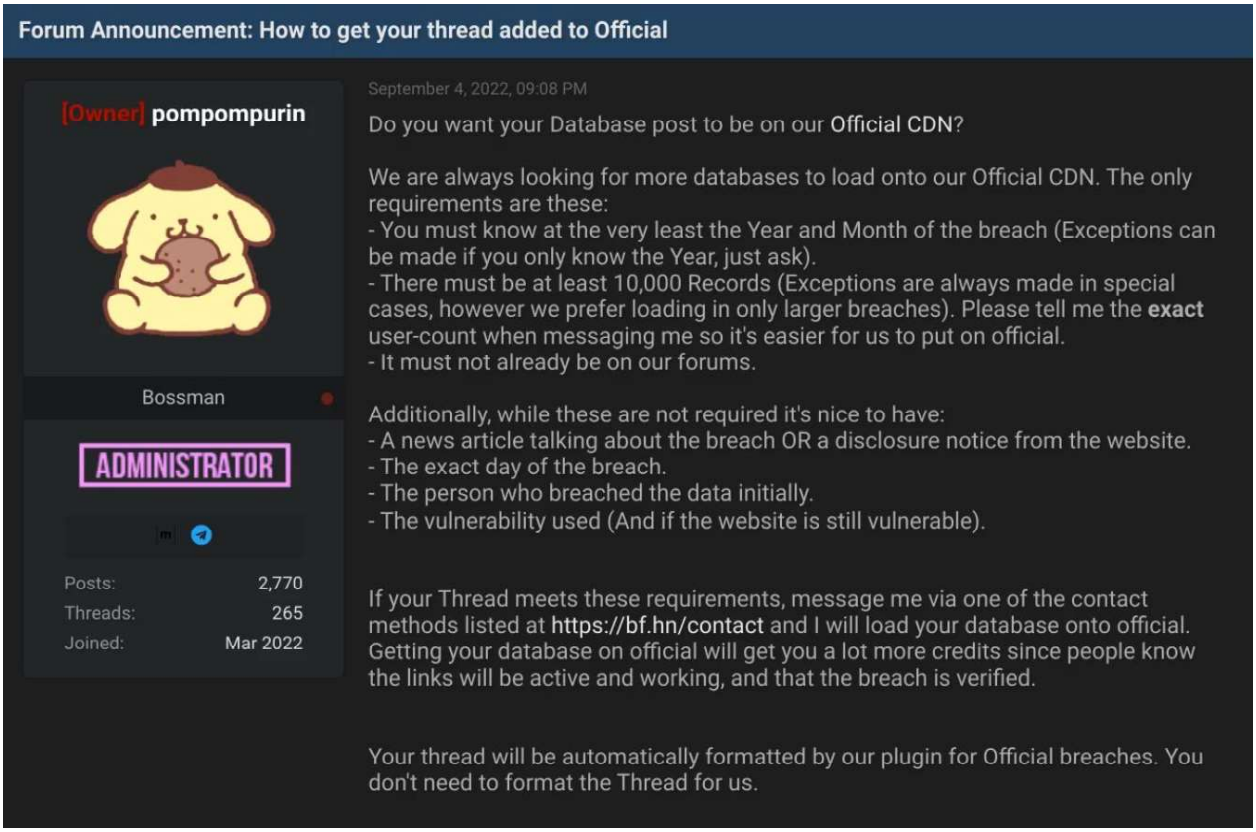


D. BreachForums "Official" Database Forum[1]

18. The "Databases" section of BreachForums includes a section titled "Official," which is described as a "Forum where databases stored on our own servers are kept. These threads are guaranteed to be online, and will not have any dead links." Official databases are available for purchase through a "credits" system administered by BreachForums. Credits are available for purchase on the site, or earned through contributing content.

19. On or about September 4, 2022, pompompurin made a post in the "Official" section detailing the process to have data posted to the site's official content distribution network ("CDN"):

[1] RaidForums had a similar setup and also offered "credits" for purchase.



20. In this post, pompompurin states that users seeking to post databases to the official BreachForums CDN must contact him directly, and that he will personally load the database to the CDN.

21. As of January 11, 2023, the Official section purported to contain 879 datasets, consisting of over 14 billion individual records. These databases include a wide variety of both U.S. and foreign companies, organizations, and government agencies. Based on a review of publicly available posts, pompompurin has personally confirmed when leaked databases are added to the Official section in at least 106 instances.

E. Pompompurin Adds Victim-2's Database to BreachForums CDN

22. In or around April 2022, a database from a U.S.-based internet hosting and security services company ("Victim-2") containing names, addresses, phone numbers, usernames, password hashes, and email addresses for approximately 8,000 customers, as well as payment card

information for approximately 1,900 customers, was posted to BreachForums. On or about May 10, 2022, the post's creator, using the moniker "agent," posted that the database had been moved to the CDN, after he/she had requested pompompurin to approve it on or about April 30, 2022. On or about September 24, 2022, pompompurin edited the post, stating "Official information edited," indicating that pompompurin had modified the link to the compromised database on the BreachForums CDN. Victim-2 has confirmed the breach and provided information to the U.S. authorities.

23. On or about October 27, 2022, a FBI online covert employee ("OCE") located in the Eastern District of Virginia purchased and downloaded this database for 8 credits. Any registered BreachForums user can purchase credits through the BreachForums website. As of October 20, 2022, credits cost approximately $0.25 each, and are available in bundles of 30, 60, 120, 240, and 500. Various forms of cryptocurrency are accepted as payment.

24. Upon review, the downloaded archive contained a text file named "Breached_Info.txt," with the following message:

> This file has been downloaded from BreachForums. Please check us out.
> Our database list is provided here: https://breached.co/databases
> > Please do the right thing, if you share this database please mention where it was downloaded from!
> At the end of the day with your help the more users we get the more high quality/private databases will be leaked.

25. The downloaded archive also contained 11 text files, most of which are structured query language ("SQL") database[2] exports that include customer names, addresses, phone numbers, usernames, password hashes, email addresses, and credit card information to include card number, expiration date, and card verification value ("cvv"), as described in the

[2] In my training and experience, a SQL database is a type of relationship database that uses structured query language for creating, modifying, and retrieving data from database tables. SQL databases are often used by forums to preserve and store information concerning activity on the forum.

BreachForums post. Review of the database by the U.S. authorities confirmed that this is the same data that Victim-2 confirmed was exfiltrated from its network.

26. Based on my training and experience, Victim 2's data downloaded from the BreachForums CDN constitutes "access devices," as defined under 18 U.S.C. § 1029(e)(1), because they are a means of account access that either could have been "used to obtain money, goods, services, or any other thing of value," or could "be used to initiate a transfer of funds." In particular, the card numbers, expiration dates, and cvvs could be used to obtain money, goods, services, and/or other things of value, or could be used to initiate a transfer of funds.

F. Pompompurin Adds Victim-3's Database to BreachForums CDN

27. Another database, purportedly obtained from a compromise of a U.S.-based investment company ("Victim-3") and containing at least 5 million customer email addresses, is also available to download from BreachForums for 8 credits. More specifically, on or about September 21, 2022, pompompurin moved this database to the BreachForums CDN, which, as stated above, means that it is available for download.

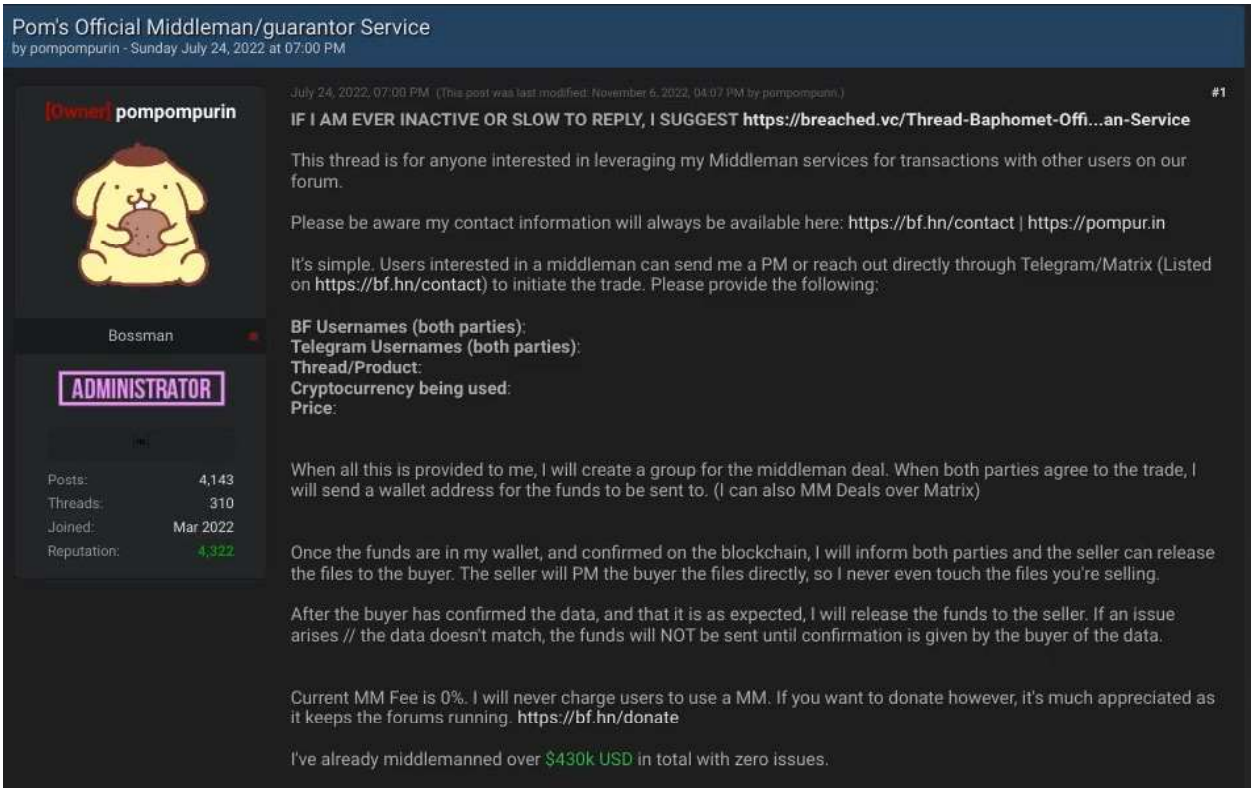
28. On October 17, 2022, a FBI OCE located in the Eastern District of Virginia purchased and downloaded this database. The downloaded archive contained an identical Breached_Info.txt file, along with a text file containing approximately 7,732,243 lines of comma-delimited text. The file contains headers including Account Owner, Account Name, Type, Last Activity, Last Modified Date, and Billing State/Province. A separate FBI investigation has verified that this data originated from a computer network compromise of Victim-3.

29. A representative for Victim-3 informed the FBI that Victim-3 customers use these identifiers when contacting Victim 3 for customer support; therefore, the compromised database can be used to execute social engineering attacks against Victim-3's customer base. In such an

attack, a malicious actor would contact Victim-3's customer support and use information from the database to impersonate a legitimate customer. After a successful impersonation attempt, the actor could then change the legitimate customer's password and thus gain access to the account. With this access, the malicious actor could transfer money from the compromised account to a bank account or debit card controlled by the actor. Based on my training and experience, I know this to be a relatively common way for fraudsters to compromise financial accounts. For these reasons, Victim 3's data downloaded from BreachForums CDN constitutes an unauthorized access device.

G. Pompompurin's "Middleman" Service

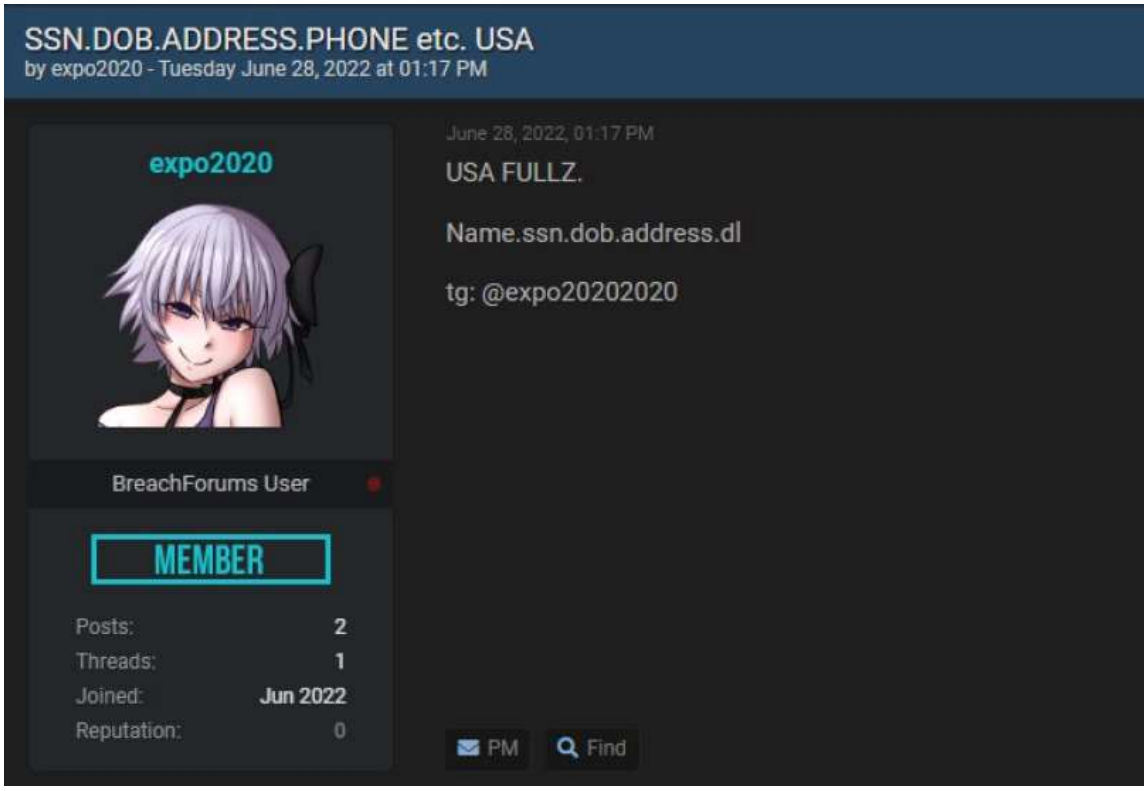
30. In addition, to facilitating transactions on the forum, BreachForums' founder pompompurin offered to act as a trusted middleman, or escrow service, between individuals on the website who sought to buy and sell information. For instance, on or about August 9, 2022, a FBI OCE reviewed a post initially made by pompompurin on BreachForums on or around July 24, 2022, and last modified on or around November 6, 2022, in which pompompurin officially announced his middleman service and explained that he would accept cryptocurrency from the purchaser and files from the seller. In the post, which is partially reflected in the below image, pompompurin stated that he has already performed over $430,000 in middleman transactions with zero issues.



31. Here, pompompurin is offering a middleman service where he enables the purchase and sale of stolen data. Pompompurin is aware of what "product" is being purchased and sold when he agrees to act as the middleman. Further, although pompompurin claims to not typically receive the files or the payment, the FBI has observed public posts in which pompompurin claims to have verified the data.

H. Pompompurin's Middleman Service is Used to Purchase PII, including Bank Account Numbers Belonging to Americans

32. On or about July 1, 2022, an OCE located in the Eastern District of Virginia reviewed the BreachForums website and observed the below depicted post made by "expo2020" on or about June 28, 2022, which offered to sell "SSN.DOB.ADDRESS.PHONE etc. USA."



33. On or about July 2, 2022, the OCE contacted expo2020 through private messages on BreachForums and the messaging application Telegram and arranged to pay approximately $500 to buy the PII and bank account information of approximately one million U.S. persons. The FBI's examination of the data sold by expo2020 revealed that it appeared to contain the PII of large numbers of U.S. persons, including their full name, e-mail address, phone number, physical address, date of birth, social security number, driver's license number, bank name, bank routing number, and bank account number.

34. Later, on or about July 2, 2022, the OCE contacted pompompurin through private messages on BreachForums and Telegram to inquire about using pompompurin's middleman service to conduct a second transaction with expo2020 in which the OCE paid approximately $5,000 to purchase the PII and bank account information of approximately 15 million U.S. persons. Pompompurin agreed to act as an escrow for the funds transfer to ensure the data purchased was

received and, on or about July 6, 2022, the OCE, pompompurin and expo2020 engaged in a Telegram group chat to complete the transaction. In this chat, the OCE stated to pompompurin that the data to be purchased should include date of birth, social security number, and bank information, stating that the information was to be used for conducting financial scams. Upon receipt of the files, the OCE confirmed to pompompurin that the data contained these elements, and pompompurin released funding to expo2020.

35. Thus far, federal law enforcement has identified 99 records that list the bank account and routing numbers for a credit union based in Virginia. Law enforcement then provided this information to the credit union for validation. The credit union examined these records and confirmed that the records contained 67 valid customer identifiers, including name and social security number, as well as valid account information.

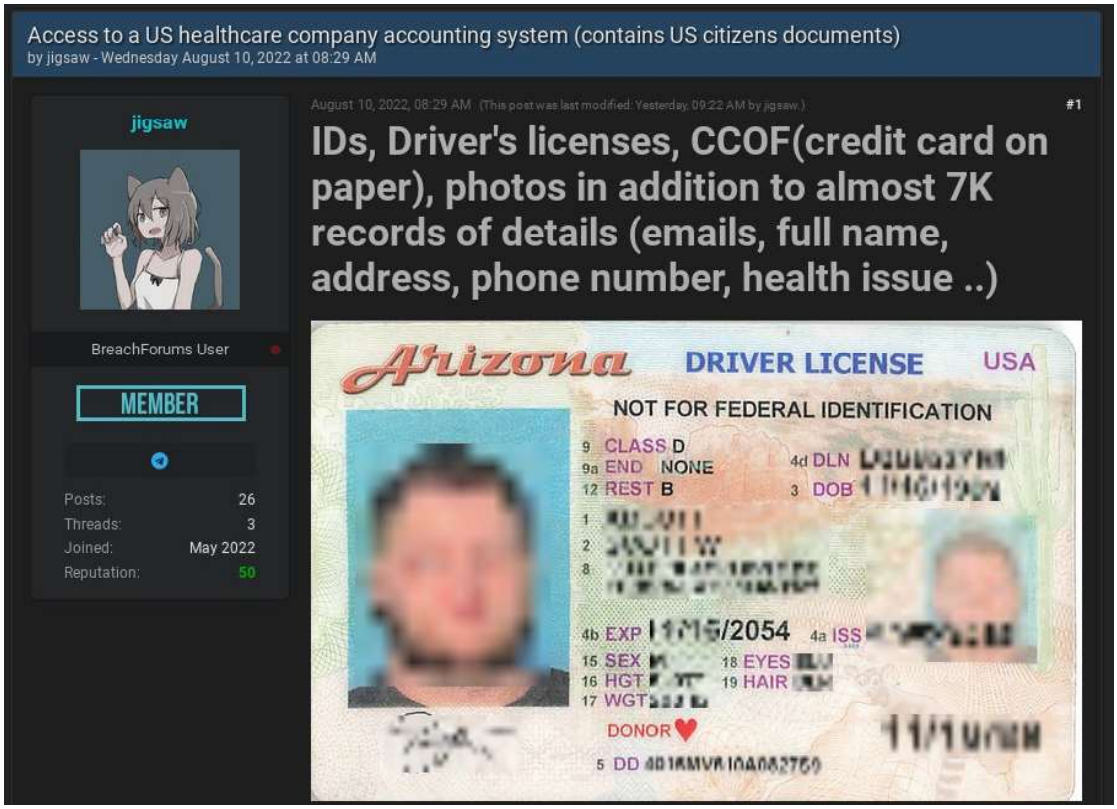
36. Based on my training and experience, the data provided by expo2020 constitutes "access devices," as defined under 18 U.S.C. § 1029(e)(1), because they are a means of account access that either could have been "used to obtain money, goods, services, or any other thing of value," or could "be used to initiate a transfer of funds." In particular, the bank information could be used to obtain money, goods, services, and/or other things of value, or could be used to initiate a transfer of funds.

I. Pompompurin's Middleman Service is Used to Transfer Victim-1 Customer Identification Documents, including Credit Card numbers

37. As explained below, the FBI's investigation indicates that through his role as a "middleman," pompompurin aided and abetted the transfer of identification documents belonging to Victim-1's customers. Further, pompompurin was aware that these documents were stolen.

38. Victim-1 is a U.S.-based company providing software to manage electronic healthcare records, medical billing records, appointment scheduling, and medical practice

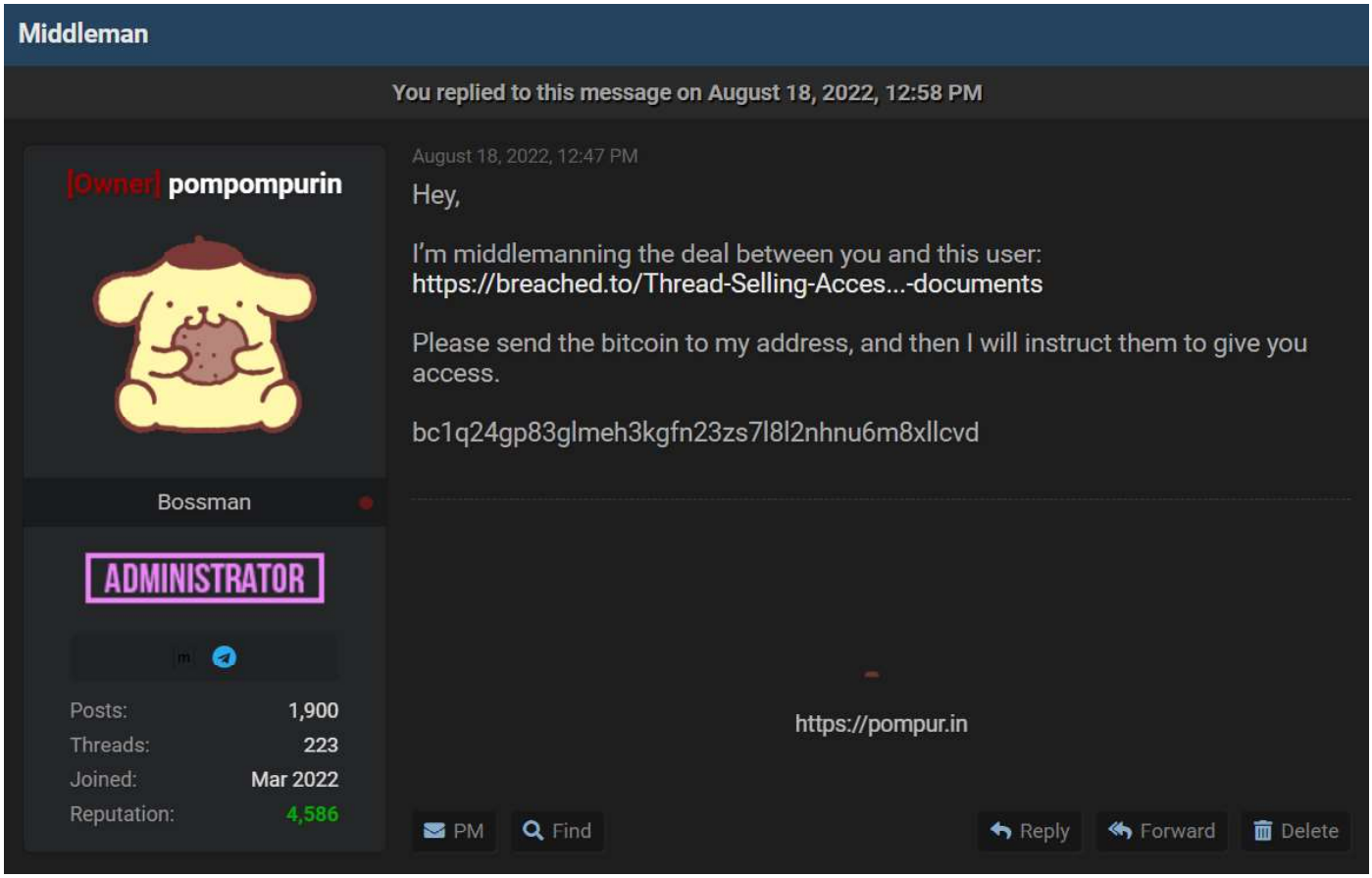
management. On or about August 17, 2022, an OCE located in the Eastern District of Virginia reviewed the BreachForums website and observed a post depicted below that was made by "jigsaw" on or about August 10, 2022. In this post, jigsaw attempted to sell "Access to a US healthcare company accounting system (contains US citizens documents)." This information purportedly included credit card numbers, emails, full names, addresses, phone numbers, and other information.



39. Later, on or about August 17, 2022, the OCE contacted jigsaw through private messages on BreachForums and Telegram and arranged for the purchase of the access to the U.S. healthcare company's system, as well as a list of additional credentials that jigsaw had stolen from Victim-1 for $3,000.

40. On or around August 18, 2022, the OCE and jigsaw arranged to have pompompurin act as a middleman for the transaction. In a private message on BreachForums, pompompurin

contacted the OCE and requested payment via Bitcoin:



41. In response, the OCE asked, "just wondering if theres [sic] a way to make sure this access actually has the IDs, card #s, and records that the description says before the money is released. The access is not very helpful for me if theres [sic] no data I can use," to which pompompurin replied, "The money wont [sic] be released until you confirm you got what you paid for."

42. In a follow-up conversation via Telegram, pompompurin assured the OCE that the funds would not be transferred to jigsaw until the OCE had confirmed his or her access to the U.S. healthcare company's accounting system:

> **OCE:** hey, just replied to your pm on breached. just curious about how mm works for buying network access…like do i get to confirm that the access actually has the credit card #s and id photographs before the btc gets released to seller? access isnt worth much

> to me without the data to make my money back lol…its this one with jigsaw https://breached.to/Thread-Selling-Access-to-a-US-healthcare-company-accounting-system-contains-US-citizens-documents
>
> **Pom:** Once you confirm you got access and got what was advertised the funds will be released…If any issues arise then it'll be figured out from there

43. After the OCE confirmed that the funds were sent to pompompurin, jigsaw provided a link to download files that included a means to gain apparent access to the U.S. Healthcare Company's account system. Jigsaw also provided a file (samples.7z) containing driver's license photos, insurance cards, and credit card on file paperwork for approximately 13 individuals, that were purportedly obtained from the victim network (credit card on file paperwork includes the patient's name, address, email address, telephone number, signature, and the last four digits of the payment card on file). The FBI has confirmed that ten Arizona driver's licenses depicted in this file were photographs of legitimate identification devices.

44. Jigsaw also provided the OCE with a text file containing usernames and passwords for two accounts on the network of Victim-1. These credentials were valid for accessing patient data and insurance profiles, as well as billing information and refund management. This access could be used by malicious actors in furtherance of identity theft and/or fraudulent insurance billing schemes, in addition to revealing sensitive healthcare information about U.S. citizens and interfering with healthcare services.

45. The U.S. authorities have confirmed with Victim-1 that both the identification documents and network access credentials are authentic data from Victim-1's network. Victim-1 has confirmed to the U.S. authorities that the credentials provided by jigsaw were valid and could be used to access documents and records for a U.S.-based healthcare provider, which are stored by Victim-1, including the information from the samples.7z file.

46. Based on my training and experience, the credentials provided by jigsaw constitute "access devices," as defined under 18 U.S.C. § 1029(e)(1), because they are a means of account access that either could have been "used to obtain money, goods, services, or any other thing of value." In particular, Victim-1 informed me that with the access provided by jigsaw, a malicious actor could change account information so that reimbursement payments could be sent to an account or address controlled by the actor, rather than the medical practice that provided care. Additionally, the personally identifiable information contained in patient records maintained by Victim-1 can be and is sold on internet sites such as BreachForums.

Recent Activity on BreachForums

47. On or about December 18, 2022, a BreachForums user with the moniker "USDoD" posted details of approximately 87,760 members of InfraGard, a partnership between the FBI and private sector companies focused on the protection of critical infrastructure. The FBI has determined that the information was obtained without authorization using a social engineering attack. Additionally, on or about January 4, 2023, information obtained from a major U.S.-based social networking site was posted by a user with the moniker "StayMad." This information included names and contact information for approximately 200 million users.

Attribution of Conor Fitzpatrick as "pompompurin"

48. As detailed below, the information available to law enforcement indicates that Conor Brian Fitzpatrick controlled and used the above-described accounts that incorporated variations on the online moniker pompompurin, including the "pompompurin" accounts on Raidforums and BreachForums. FITZPATRICK currently lives at a residence located on Union Avenue in Peekskill, New York ("the UNION PREMISES").

49. As mentioned above, in or around February 2022, law enforcement seized RaidForums and the website was taken offline. As part of the investigation, pursuant to mutual legal assistance requests, the FBI obtained images of servers controlled by RaidForums that, among other things, contained a SQL database of forum activity. TheRaidForums database included communications between the RaidForums administrator, using the moniker "omnipotent," and pompompurin, as well as pompompurin's RaidForums logins and subscriber information.

50. In reviewing the RaidForums logs, the FBI determined that the pompompurin user account was accessed from the following IP addresses that resolve to Verizon Communications:

- 2600:1017:b017:810f:5899:2deb:d428:647e at 4/24/21 7:10:35 PM UTC
- 2600:1017:b01e:d0b9:a9ee:1962:532a:8189 at 3/13/21 6:34:21 PM UTC
- 2600:1017:b801:325f:a0e9:c125:d43:c55c at 5/10/21 1:58:21 PM UTC
- 2600:1017:b803:ee00:905e:faa5:6358:3e1e at 1/28/21 2:52:03 PM UTC
- 2600:1017:b805:a362:1cb4:629f:d864:c3fd at 3/13/21 5:45:03 PM UTC
- 2600:1017:b807:6e9f:bc44:9732:6093:6eb8 at 5/7/21 1:12:57 PM UTC
- 2600:1017:b809:4d0e:fdbb:731:688:60f1 at 5/14/21 2:02:45 PM UTC
- 2600:1017:b809:d414:39d1:91e0:f47f:a2a3 at 6/3/21 1:50:07 PM UTC
- 2600:1017:b80b:7b0d:2c23:576d:bf0e:d6a6 at 6/26/21 1:18:36 AM UTC
- 2600:1017:b80f:176c:2511:9868:a34e:a887 at 4/19/21 2:43:25 PM UTC
- 2600:1017:b80f:b59a:e04c:5f44:856f:7b3a at 4/26/21 4:56:13 PM UTC
- 2600:1017:b813:4109:d432:5151:87f1:3ae at 6/8/21 2:02:27 PM UTC
- 2600:1017:b816:7439:1dbb:f4d5:3999:fde2 at 6/18/21 2:04:44 PM UTC
- 2600:1017:b816:7439:1dbb:f4d5:3999:fde2 at 6/18/21 2:04:45 PM UTC
- 2600:1017:b816:8011:a9a7:6b38:bb16:7f3 at 3/22/21 2:01:50 PM UTC
- 2600:1017:b818:e5a5:5cce:8ac0:d1a7:fe62 at 3/23/21 1:59:09 PM UTC
- 2600:1017:b81a:6abb:d82c:36ce:49a1:f775 at 4/15/21 6:11:38 PM UTC
- 2600:1017:b81c:8f96:ac00:8940:3a23:7d5e at 4/6/21 3:30:32 PM UTC
- 2600:1017:b81d:9854:3170:73b3:11ac:fed4 at 3/9/21 4:07:06 PM UTC
- 2600:1017:b81e:dfc9:2d11:bbe9:279d:9e67 at 5/27/21 3:37:08 PM UTC
- 2600:1017:b81e:fc04:ed38:d4f3:6a74:a2f at 5/6/21 2:02:14 PM UTC
- 2600:1017:b81e:fc04:ed38:d4f3:6a74:a2f at 5/6/21 2:02:14 PM UTC
- 2600:1017:b823:291f:8b5:e404:b7ff:7b5e at 5/3/21 1:57:44 PM UTC
- 2600:1017:b825:1a49:6841:4f98:2b5f:2dfe at 3/15/21 2:40:23 PM UTC
- 2600:1017:b828:2b01:9517:406:35ea:916e at 5/7/21 1:52:00 PM UTC
- 2600:1017:b829:a42e:a0aa:8d3d:95b6:c592 at 4/22/21 2:48:47 PM UTC
- 2600:1017:b82d:b89c:59fc:f2f0:cc82:2dcd at 5/25/21 1:58:06 PM UTC

- 2600:1017:b82f:118e:d11a:a805:fc0e:d8cb at 5/27/21 2:07:23 PM UTC
- 2600:1017:b82f:118e:d11a:a805:fc0e:d8cb at 5/27/21 2:07:23 PM UTC
- 2600:1017:b8a1:e4b1:e954:7d46:d832:9c6b at 6/11/21 2:44:22 PM UTC
- 2600:1017:b8a3:ef0c:24fe:ec4:f550:2c25 at 7/24/21 3:54:13 PM UTC
- 2600:1017:b8a8:c1db:bd1e:ae7c:841e:aa8c at 1/27/21 3:45:47 PM UTC
- 2600:1017:b8a9:26bf:5d42:2704:807f:ba69 at 6/1/21 2:07:53 PM UTC
- 2600:1017:b8aa:6b75:4152:414b:4c2:5841 at 2/8/21 2:55:25 PM UTC
- 2600:1017:b8aa:ae19:cc03:388c:73da:89d8 at 7/9/21 10:37:26 PM UTC
- 2600:1017:b8aa:c86:ec22:d372:eab0:569b at 3/2/21 3:43:47 PM UTC

51. Records received from Verizon, in turn, revealed that at least nine of the above IP addresses[3] used to access the pompompurin account on RaidForums were, at the time, associated with the following mobile devices registered to "Conor Fitzpatrick" at the UNION PREMISES with a cell phone number ending in 3144 ("the 3144 Verizon Telephone Number").

IMSI: 311480405756028
IMEI: 353888106005342 (iPhone 11 Pro Max), 356697089909371 (iPhone 7 Plus)

52. The RaidForums records also contained the following communication between pompompurin and omnipotent on or about November 28, 2020, in which pompompurin specifically mentions to omnipotent that he had searched for the e-mail address conorfitzpatrick02@gmail.com and name "conorfitzpatrick" within a database of breached data from "ai.type":

> [Quoting "pompompurin":]
>
> Hello, I'm sorry to bother you with this but I noticed recently that the ai.type databreach post doesn't seem to include every user (?) at least to my understanding. Looking up one of my old emails on HIBP, I come up as in it, but I cannot locate myself in the file provided at https://raidforums.com/Thread-ai-type-Database-Leaked-Download-Exclusive
>
> It seems that maybe it is only a partial amount of data from it? I was under the impression that it was the full amount of data from looking at the thread as I didn't see any mention of it only being "some" of the data from the breach.

[3] No data was available for the remaining 27 IP addresses due to data retention limitations at Verizon.

> Not messaging to ask for credits back or anything, because I wanted it anyways, I just wanted to let you know that it doesn't seem to be the full amount of data and that the thread doesn't seem to communicate that it isn't the full one.
>
> Thanks ;)
>
> [Quoting "Omnipotent":]
>
> What email did you look up and how?
>
> [Quoting "pompompurin:]
>
> Apologies for late reply, here is another email that I found to be present on HIBP, but not inside of the file provided on the thread (I don't want to share my actual email for obvious reasons, but this email seems to have the same case as mine):
> conorfitzpatrick02@gmail.com
> https://a.pomf.cat/vvxevp.png (backup: https://archive.is/uYiTq)
>
> To search the file, I used the command "grep -i 'conorfitzpatrick' aitype.txt"
> To make sure the command is working correctly, I made a test.txt file including the email address I am trying to search in the same format as the data in the breach. Then, I ran the same exact command against the test file and it was able to find the email. (I also did a second search on the test.txt where I made some letters capital, to show I was doing a case insensitive search against the data)
> https://a.pomf.cat/dstqbv.png (backup: https://archive.vn/dOKnf)

53. As widely reported in the media, the company "ai.type" was the victim of a breach of its database[4] in or around December 2017. In the above communication, pompompurin stated he had looked "up one of [his] old emails on" the website "Have I Been Pwned"[5] (or "HIBP" for short) to confirm his e-mail was part of the breach, but pompompurin could *not* find it in the ai.type breach data he had purchased on RaidForums — suggesting that the RaidForums ai.type database

[4] "The emails, phone numbers, and locations of 31 million users of Android keyboard app Ai.type have been compromised after the developer failed to secure the server on which the information was stored. Some 577 gigabytes of data is said to have been exposed, representing more than three quarters of the app's total userbase." See "Ai.type keyboard app developer accidentally leaks personal data of 31 million users" by Scott Scrivens, December 7, 2017 at Ai.type keyboard app developer accidentally leaks personal data of 31 million users (androidpolice.com), last accessed on October 3, 2022.

[5] Per Have I Been Pwned at https://haveibeen pwned.com, the website Have I Been Pwned allows people to search across multiple collected data breaches to see if their e-mail or phone number had been compromised. You can enter your own e-mail address or phone number and the website will respond with which data breaches they have been seen in.

was incomplete. Pompompurin then suggested that maybe it was a "partial amount of data," but explained that he was under the impression that it was the full amount of data. Pompompurin then says that he is not looking for a refund, but just wanted to communicate to omnipotent that the ai.type stolen database that had been listed for sale on RaidForums was not the full database, and that this should be better communicated ("Not messaging to ask for credits back or anything, because I wanted it anyways, I just wanted to let you know that it doesn't seem to be the full amount of data and that the thread doesn't seem to communicate that it isn't the full one. Thanks 😉").

54. Omnipotent responded to pompompurin with the question "What email did you look up and how?"

55. In a reply, pompompurin then mentioned "conorfitzpatrick02@gmail.com" as an e-mail he had searched in "HIBP," but was not able to locate in the stolen ai.type database. In this conversation with omnipotent, pompompurin claimed that he did not want to share his "actual email for obvious reasons," but described the conorfitzpatrick02@gmail.com as an e-mail that "seems to have the same case" as his actual e-mail address. Further, pompompurin stated that he had searched the name "conorfitzpatrick" in the RaidForums version of the ai.text database using a "grep" command, and even had run this command against a test file he had created.

56. Although pompompurin's above-described correspondence appears to suggest that conorfitzpatrick02@gmail.com was not his "actual email address," there are several reasons why I believe that pompompurin (i) searched "conorfitzpatrick" because conorfitzpatrick02@gmail.com was indeed his old email address and contained his own name; and (ii) purchased the ai.type database to see whether, among other things, his replacement email for conorfitzpatrick02@gmail.com was exposed in the data breach.

57. As an initial matter, in my training and experience, hackers commonly search themselves in databases to identify any vulnerabilities they might have and determine if any of their personal information may be accessible online.

58. Further, records received from Google indicate that, in the months preceding pompompurin's correspondence with omnipotent, FITZPATRICK appears to have registered a Google account with the email address conorfitzpatrick2002@gmail.com to replace the older email address (conorfitzpatrick02@gmail.com) that pompompurin had identified. For instance, according to records from Google, the conorfitzpatrick2002@gmail.com Google account was registered on or about May 26, 2019, and the Google account associated with conorfitzpatrick02@gmail.com was then closed on or about April 8, 2020. In addition, the Google Pay accounts linked to the conorfitzpatrick2002@gmail.com and conorfitzpatrick02@gmail.com accounts were both registered under the name "Conor Fitzpatrick," and listed the UNION PREMISES and the 3144 Verizon Telephone Number as contact information. As described above, the 3144 Verizon Telephone Number was linked to nine IP addresses that accessed pompompurin's account on RaidForums. The Google Pay account associated with conorfitzpatrick2002@gmail.com also listed a Visa credit card ending in 3068 with an expiration date of May 2027 (5/2027).

59. The FBI also searched the email addresses conorfitzpatrick2002@gmail.com and conorfitzpatrick02@gmail.com on the website https://haveibeenpwned.com/ to determine if they were included in the breached ai.type database. As pompompurin appeared to indicate, the results of the queries indicated that the "old" conorfitzpatrick02@gmail.com email address was in the database. The newer conorfitzpatrick2002@gmail.com email address was not.

60. Additional records received from Google further tie the user of the conorfitzpatrick2002@gmail.com to FITZPATRICK and the moniker pompompurin. For instance, the recovery email address for conorfitzpatrick2002@gmail.com was funmc59tm@gmail.com. Subscriber records for this account reveal that the account was registered under the name "a a,"[6] and created on or about December 28, 2018 from the IP address 74.101.151.4.[7]

61. Records received from Verizon, in turn, revealed that IP address 74.101.151.4 was registered to a customer with the last name FITZPATRICK[8] at the UNION PREMISES with a telephone number ending in 2956, and an email address that is associated with this same person's public employment. According to public records reviewed by the FBI, the person with the last name Fitzpatrick resides at the UNION PREMISES with another individual with the last name Fitzpatrick and FITZPATRICK. Based on public records reviewed by the FBI, as well as the age difference, and their shared habitation of the UNION PREMISES, I believe that the person with the last name Fitzpatrick is FITZPATRICK's father.

62. Records received from Google concerning conorfitzpatrick2002@gmail.com also showed logins from numerous virtual private network (VPN) provider companies from at least on or about September 20, 2021 through on or about May 12, 2022, including M247 Ltd, Datacamp Limited, Tzulo, Performive, Blix Solutions, Sharktech, Hosting Services Inc, QuadraNet, IVPN, and Mullvad. Based on the timing and variety of VPNs, as well as my training and experience, I

[6] In my training and experience, it is common for cybercriminals to obscure their identities by registering accounts under false names, such as "a a."

[7] Google returns describe the IP address as the "Terms of Service" IP address. In my training and experience, that refers to the IP address used to create the account.

[8] I have not included the first name in order to comply with the Local Rules requirement, which mandates that parties should not use the names of uncharged individuals in public documents.

believe the user of the conorfitzpatrick2002@gmail.com Google account used multiple different VPNs to obscure his or her location and true IP address.

63. Records obtained by the FBI reveal overlaps between the IP addresses and VPN services used to access the conorfitzpatrick2002@gmail.com Google account and certain online accounts with the "pompompurin" moniker.

64. For instance, on or about March 7, 2022, records received from Google showed that the conorfitzpatrick2002@gmail.com Google account was accessed from IP address 89.187.181.117 on or about March 7, 2022. IP address 89.187.181.117 was owned by Datacamp Limited. However, a query of this IP address on Spur.us, in turn, revealed that this IP address was actually used by the VPN provider IVPN at the time. According to records from Zoom, this IP address was used the following day, on or about March 8, 2022, to log into a Zoom account under the name of "pompompurin" with an e-mail address of pompompurin@riseup.net. The pompompurin@riseup.net email address is notable because, at the time of the Zoom account's creation, it served as pompompurin's registration email address on RaidForums, per records obtained by the FBI in that investigation.

65. Further, according to the RaidForums SQL database of forum activity, IP addresses 192.252.212.39 and 89.45.224.27 were also both used to log into the "pompompurin" account on RaidForums. Indeed, of the 31 unique IP addresses logged as having been used to access the conorfitzpatrick2002@gmail.com from on or about September 20, 2021 through on or about May 12, 2022, 12 of them were also used to log into pompompurin's RaidForums account.

66. Records received from Purse.io, a cryptocurrency exchange used to purchase products online, reveal that four of the IP addresses[9] used to access the

[9] The IP addresses were 212.103.48.197, 2a0d:5600:24:a80::a77e, 37.19.206.108, and 2607:9000:4000:17::b85e.

conorfitzpatrick2002@gmail.com Google account and pompompurin's RaidForums account were also used to log into a Purse.io cryptocurrency account that was registered to "Conor Fitzpatrick" with the email address conorfitzpatrick2002@gmail.com from on or about March 14, 2022, through on or about April 27, 2022 (the "Conor Fitzpatrick Purse.io account"). These IP addresses were owned by the providers M247 Ltd, Datacamp Limited, and Tzulo at the time. However, a lookup on Spur.us shows that the 212.103.48.197 IP address (M247 Ltd) and 37.19.206.108 IP address (Datacamp Limited) were both utilized by VPN provider IVPN.

67. In my training and experience, the repeated use of common virtual private servers and VPN providers, including four of the same IP addresses, suggests that these accounts were likely controlled by a common person.

68. Records received from Purse.io also show that the Conor Fitzpatrick Purse.io account purchased several items in or around 2022 that were delivered to the UNION PREMISES with the 3144 Verizon Telephone Number.[10] Further, the Conor Fitzpatrick Purse.io account also reveals additional ties between that account holder and the user of the pompompurin account on RaidForums. For instance, in total, seven of the nine unique IP addresses that logged into the Conor Fitzpatrick Purse.io account also logged into pompompurin's account on RaidForums. In addition, the Conor Fitzpatrick Purse.io account was funded exclusively by a Bitcoin address that pompompurin had discussed in posts on RaidForums.

69. Also, records obtained from the SQL database of forum activity on BreachForums revealed that the pompompurin account on BreachForums was accessed from IP address 69.115.201.194 on or about June 27, 2022. That is notable because records received from Optimum Online, an Internet service provider, revealed that this IP address was registered under

[10] The account also caused purchases that were delivered to an address in Manassas, Virginia.

the name of FITZPATRICK's apparent father at the UNION PREMISES from on or about November 17, 2021 through on or about November 1, 2022. According to subscriber information provided by Optimum Online, this account was registered with two email addresses hosted at optimum.net. One of the registration email addresses appeared to incorporate FITZPATRICK's name (conorfitz@optimum.net), while the other incorporated the name of his suspected father.

70. In my training and experience, I know that cyber criminals use a variety of methods to obscure their IP addresses, such as utilizing VPN services or The Onion Router (Tor).[11] However, these services are occasionally misconfigured and expose the user's true IP address. Accordingly, while the FBI's examination of the BreachForums database reveals that the pompompurin account was typically accessed through VPN services or Tor, I believe it is notable that IP address 69.115.201.194 was once used to login to the pompompurin account on or about June 27, 2022.

71. Further, records received from Apple Inc. concerning an iCloud account associated with FITZPATRICK reveals that the account was accessed approximately 97 times from IP address 69.115.201.194 between on or about May 19, 2022 and on or about June 2, 2022, from an iPhone mobile device.

72. The FBI's examination of the pompompurin account's posting activity on RaidForums and BreachForums further suggests that they've been controlled by a common user. For instance, in a post titled "Welcome & FAQ Thread" on BreachForums on or about March 16, 2022, pompompurin posted, "I've created this forum as an alternative to RaidForums since it was seized…If you used RaidForums you most likely remember me, I was one of the more active users on there."

[11] In my training and experience, Tor is a free and open-source software for enabling anonymous communication.

73. Further, the pompompurin account on BreachForums has alluded to past activity by the pompompurin account on RaidForums. For example, on or about July 4, 2022, the pompompurin account on BreachForums created a post titled "Capital Economics Database – Leaked, Download!" The post included the following description:

> In December 2020, the economic research company Capital Economics suffered a data breach that exposed 263k customer records. The exposed data included email and physical addresses, names, phone numbers, job titles and the employer of impacted customers. Funny story about this, ***when I originally posted this on RaidForums in 2020***[,] some Russian stole it and tried to sell it on exploit.in."

(Emphasis added).

74. The post is notable because, on or about January 4, 2021, pompompurin created a post on RaidForums titled "[capitaleconomics.com] 263,630 Users." The post stated, in relevant part, "Website: https://www.capitaleconomics.com..Dumped by me on 12/12/2020…," and included a link to download the compromised data.

75. On or about October 26, 2022, an FBI OCE observed the user profile of the pompompurin account at a time it was logged into BreachForums.[12] At the same time, an FBI agent reviewed records reflecting the physical location of the telephone associated with FITZPATRICK's 3144 Verizon Telephone Number, which was obtained from Verizon Wireless pursuant to a cell phone GPS warrant obtained in a parallel investigation out of the Northern District of California. These results, accurate to within approximately 1 kilometer, indicate that while accessing BreachForums, FITZPATRICK was likely physically located around the area of the UNION PREMISES.

[12] Based on the investigation, I understand that BreachForums profiles indicate whether a user is currently logged into the website.

76. Further, while performing physical surveillance of the UNION PREMISES on or about February 6, 2023, FBI and HHS-OIG agents observed that the pompompurin account was active on BreachForums while FITZPATRICK was inside the UNION PREMISES.

77. In view of the above, I believe that FITZPATRICK has used the same VPNs and IP addresses to log into the e-mail account conorfitzpatrick2002@gmail.com, the Conor Fitzpatrick Purse.io account, the pompompurin account on RaidForums, and the pompompurin account on BreachForums, among other accounts. There is also probable cause to believe that FITZPATRICK is the same individual who does and has used the moniker pompompurin on RaidForums and BreachForums to perform the above-described acts.

Court Authorized Search of Fitzpatrick's Residence on March 15, 2023

78. On March 15, 2023, law enforcement executed a court-authorized search of the residence that FITZPATRICK shares with his family. After advising FITZPATRICK of his constitutional rights, FITZPATRICK waived his rights and agreed to speak with law enforcement. During the subsequent interview, FITZPATRICK admitted that he is the user of the pompompurin account. He also admitted that he owns and administers BreachForums and previously operated the pompompurin account on RaidForums. He stated that after RaidForums was seized by law enforcement, he was approached by individuals who thought he would be competent enough to run a similar site. FITZPATRICK stated that he agreed to do so.

79. FITZPATRICK admitted that he is aware that BreachForums is a site where people can and do solicit the purchase and sale of compromised data. He also stated that he operates a middleman service and he estimated that he conducts 2-3 such transactions a day. He further admitted that these transactions involve the purchase and sale of compromised data. FITZPATRICK stated that he does not charge for the middleman service, but he does charge for

credits and membership upgrades on BreachForums. He estimated that he earned approximately $1,000 a day from BreachForums, and that he uses this money to administer BreachForums and purchase other domains.

CONCLUSION

80. Based on the forgoing, I submit there is probable cause to support that from in or around March 2022 to the present, in Prince William County, Virginia, within the Eastern District of Virginia and elsewhere, CONOR BRIAN FITZPATRICK, did knowingly and with the intent to defraud, combine, conspire, confederate and agree with other persons to commit and aid and abet the following offense:

a. Without the authorization of the issuers of access devices, knowingly and with the intent to defraud, solicit individuals with the purpose of selling unauthorized access devices, to wit bank routing and account numbers, social security numbers, credit card numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States entities, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(6).

All in violation of Section 1029(b)(2).

Respectfully submitted,

John Longmire
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to in accordance with Fed. R. Crim. P. 4.1 by telephone on the ____ day of March, 2023.

John F. Anderson Digitally signed by John F. Anderson
Date: 2023.03.15 19:55:00 -04'00'

Hon. John F. Anderson
UNITED STATES MAGISTRATE JUDGE